

Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

1 1. (currently amended) An apparatus for securely authenticating a
2 data exchange session with an implantable medical device, comprising:
3 a secure key repository comprising a memory and configured to maintain
4 a crypto key uniquely associated with an implantable medical device to
5 authenticate data during a data exchange session; and
6 an external device configured to establish a secure connection through a
7 short range interface with the secure key repository, to authenticate authorization
8 to access data on the implantable medical device by securely retrieving the crypto
9 key from the secure key repository, and to transact the data exchange session
10 using the crypto key to authenticate the data by transitioning to a long range
11 interface.

1 Claim 2 (cancelled).

1 3. (previously presented) An apparatus according to Claim 1, further
2 comprising:
3 an authentication component configured to employ the crypto key during
4 the data exchange session, comprising at least one of:
5 a command authenticator configured to authenticate commands
6 exchanged through the external device with the implantable medical device and;
7 a data integrity checker configured to check the integrity of the
8 data received by and transmitted from the external device; and
9 a data encrypter configured to encrypt the data received by and
10 transmitted from the external device.

1 4. (previously presented) An apparatus according to Claim 1, further
2 comprising:

3 a short range interface logically defining a secured area around the
4 implantable medical device in which to establish the secure connection; and
5 a long range interface logically defining a non-secured area extending
6 beyond the secured area in which to transact the data exchange session.

1 5. (previously presented) An apparatus according to Claim 1, further
2 comprising:

3 a key generator configured to statically generate the crypto key, and to
4 persistently store the crypto key in the secure key repository.

1 6. (previously presented) An apparatus according to Claim 5, wherein
2 the crypto key is stored on at least one of the implantable medical device, a
3 patient designator, a secure database, a physical token, and a repeater.

1 7. (previously presented) An apparatus according to Claim 5, wherein
2 the crypto key is securely retrieved from the secure key repository through a
3 programmer.

1 8. (previously presented) An apparatus according to Claim 1, further
2 comprising:
3 a key generator configured to dynamically generate the crypto key.

1 9. (previously presented) An apparatus according to Claim 8, wherein
2 the crypto key is stored on at least one of the implantable medical device, a
3 patient designator, and a repeater.

1 10. (previously presented) An apparatus according to Claim 8, wherein
2 the crypto key is securely retrieved from the secure key repository through at least
3 one of a programmer and a repeater.

1 11. (previously presented) An apparatus according to Claim 1, wherein
2 the crypto key is maintained on the implantable medical device, further
3 comprising:

4 a short range telemetry interface retrieving the crypto key through short
5 range telemetry.

1 12. (previously presented) An apparatus according to Claim 11,
2 wherein the short range telemetry comprises inductive telemetry.

1 13. (previously presented) An apparatus according to Claim 11,
2 wherein the external device comprises a programmer.

1 14. (previously presented) An apparatus according to Claim 13,
2 wherein the crypto key is provided from the programmer to a repeater.

1 15. (previously presented) An apparatus according to Claim 11,
2 wherein the external device comprises a patient designator.

1 16. (previously presented) An apparatus according to Claim 15,
2 wherein the crypto key is provided from the patient designator to at least one of a
3 programmer and a repeater.

1 17. (previously presented) An apparatus according to Claim 1, further
2 comprising:

3 a secure database configured to maintain the crypto key; and

4 a secure server configured to provide the crypto key through a secure
5 connection.

1 18. (previously presented) An apparatus according to Claim 17,
2 wherein the secure connection comprises at least one of a serial or hardwired
3 connection and a secure network connection.

1 19. (previously presented) An apparatus according to Claim 17,
2 wherein the external device comprises a programmer.

1 20. (previously presented) An apparatus according to Claim 19,
2 wherein the crypto key is provided from the programmer to a repeater.

1 21. (previously presented) An apparatus according to Claim 1, further
2 comprising:
3 a physical token configured to maintain the crypto key; and
4 a reader configured to retrieve the crypto key by accessing the physical
5 token.

1 22. (previously presented) An apparatus according to Claim 21, further
2 comprising:
3 a physical label configured to specify the crypto key on the physical token.

1 23. (previously presented) An apparatus according to Claim 22,
2 wherein the physical label comprises at least one of alphanumeric text, bar
3 coding, and an outwardly-appearing indication.

1 24. (previously presented) An apparatus according to Claim 21, further
2 comprising:
3 internal storage configured to specify the crypto key on the physical token.

1 25. (previously presented) An apparatus according to Claim 24,
2 wherein the internal storage comprises at least one of a transistor, a memory
3 circuit, an electronically readable storage medium, and a magnetically readable
4 storage medium.

1 26. (previously presented) An apparatus according to Claim 21,
2 wherein the physical token is accessed using magnetic, optical, serial, and
3 physical reading.

1 27. (previously presented) An apparatus according to Claim 1, wherein
2 the crypto key comprises at least one of a 128-bit crypto key and a symmetric
3 crypto key.

1 28. (previously presented) An apparatus according to Claim 1, wherein
2 the crypto key comprises at least one of a statically generated and persistently
3 stored crypto key, dynamically generated and persistently stored crypto key, a
4 dynamically generated and non-persistently stored session crypto key.

1 29. (previously presented) An apparatus according to Claim 1, wherein
2 the implantable medical device comprises at least one of an implantable cardiac
3 device, neural stimulation device, and drug therapy dispensing device.

1 30. (previously presented) A method for securely authenticating a data
2 exchange session with an implantable medical device, comprising:
3 maintaining a crypto key uniquely associated with an implantable medical
4 device in a secure key repository to authenticate data during a data exchange
5 session;
6 establishing a secure connection through a short range interface from an
7 external source with the secure key repository;
8 authenticating authorization to access data on the implantable medical
9 device by securely retrieving the crypto key from the secure key repository; and
10 transacting the data exchange session using the crypto key to authenticate
11 the data by transitioning to a long range interface.

1 Claim 31 (cancelled).

1 32. (previously presented) A method according to Claim 30, further
2 comprising:
3 employing the crypto key during the data exchange session, comprising at
4 least one of:

5 authenticating commands exchanged through the external source
6 with the implantable medical device and;
7 checking the integrity of the data received by and transmitted from
8 the external source; and
9 encrypting the data received by and transmitted from the external
10 source.

1 33. (original) A method according to Claim 30, further comprising:
2 logically defining a secured area around the implantable medical device in
3 which to establish the secure connection; and
4 logically defining a non-secured area extending beyond the secured area in
5 which to transact the data exchange session.

1 34. (original) A method according to Claim 30, further comprising:
2 statically generating the crypto key; and
3 persistently storing the crypto key in the secure key repository.

1 35. (original) A method according to Claim 34, wherein the crypto key
2 is stored on at least one of the implantable medical device, a patient designator, a
3 secure database, a physical token, and a repeater.

1 36. (original) A method according to Claim 35, further comprising:
2 securely retrieving the crypto key from the secure key repository through a
3 programmer.

1 37. (original) A method according to Claim 30, further comprising:
2 dynamically generating the crypto key.

1 38. (original) A method according to Claim 37, wherein the crypto key
2 is stored on at least one of the implantable medical device, a patient designator,
3 and a repeater.

1 39. (original) A method according to Claim 37, further comprising:

2 securely retrieving the crypto key from the secure key repository through
3 at least one of a programmer and a repeater.

1 40. (original) A method according to Claim 30, further comprising:
2 maintaining the crypto key on the implantable medical device; and
3 retrieving the crypto key through short range telemetry.

1 41. (original) A method according to Claim 40, wherein the short
2 range telemetry comprises inductive telemetry.

1 42. (original) A method according to Claim 40, wherein the external
2 source comprises a programmer.

1 43. (original) A method according to Claim 42, further comprising:
2 providing the crypto key from the programmer to a repeater.

1 44. (original) A method according to Claim 40, wherein the external
2 source comprises a patient designator.

1 45. (original) A method according to Claim 44, further comprising:
2 providing the crypto key from the patient designator to at least one of a
3 programmer and a repeater.

1 46. (original) A method according to Claim 30, further comprising:
2 maintaining the crypto key in a secure database; and
3 retrieving the crypto key through a secure connection.

1 47. (original) A method according to Claim 46, wherein the secure
2 connection comprises at least one of a serial or hardwired connection and a secure
3 network connection.

1 48. (original) A method according to Claim 46, wherein the external
2 source comprises a programmer.

1 49. (original) A method according to Claim 48, further comprising:

2 providing the crypto key from the programmer to a repeater.

1 50. (original) A method according to Claim 30, further comprising:
2 maintaining the crypto key on a physical token; and
3 retrieving the crypto key by accessing the physical token.

1 51. (original) A method according to Claim 50, further comprising:
2 specifying the crypto key on the physical token using a physical label.

1 52. (original) A method according to Claim 51, wherein the physical
2 label comprises at least one of alphanumeric text, bar coding, and an outwardly-
3 appearing indication.

1 53. (original) A method according to Claim 50, further comprising:
2 specifying the crypto key on the physical token using internal storage.

1 54. (original) A method according to Claim 53, wherein the internal
2 storage comprises at least one of a transistor, a memory circuit, an electronically
3 readable storage medium, and a magnetically readable storage medium.

1 55. (original) A method according to Claim 50, further comprising:
2 accessing the physical token using magnetic, optical, serial, and physical
3 reading.

1 56. (original) A method according to Claim 30, wherein the crypto key
2 comprises at least one of a 128-bit crypto key and a symmetric crypto key.

1 57. (original) A method according to Claim 30, wherein the crypto key
2 comprises at least one of a statically generated and persistently stored crypto key,
3 dynamically generated and persistently stored crypto key, a dynamically
4 generated and non-persistently stored session crypto key.

1 58. (previously presented) A method according to Claim 30, wherein
2 the implantable medical device comprises at least one of an implantable cardiac
3 device, neural stimulation device, and drug therapy dispensing device.

1 59. (previously presented) An apparatus for securely authenticating a
2 data exchange session with an implantable medical device, comprising:

3 means for maintaining a crypto key uniquely associated with an
4 implantable medical device in a secure key repository to authenticate data during
5 a data exchange session;

6 means for establishing a secure connection through a short range interface
7 from an external device with the secure key repository;

8 means for authenticating authorization to access data on the implantable
9 medical device by means for securely retrieving the crypto key from the secure
10 key repository; and

11 means for transacting the data exchange session using the crypto key to
12 authenticate the data by transitioning to a long range interface.

1 60. (previously presented) An apparatus for securely transacting a data
2 exchange session with an implantable medical device, comprising:

3 a short range interface device configured to provide communication with
4 an implantable medical device by authenticating access to a securely maintained
5 crypto key using a short range interface; and

6 an external device configured to commence a data exchange session with
7 the implantable medical device via a long range interface upon successful access
8 authentication, and to transact the data exchange session using the crypto key.

1 61. (previously presented) An apparatus according to Claim 60,
2 wherein the implantable medical device maintains patient health information in an
3 encrypted form.

1 62. (previously presented) An apparatus according to Claim 60,
2 wherein the access authentication occurs through short range telemetry, further
3 comprising:
4 a short range telemetric connection with the implantable medical device;
5 a short range telemetric device configured to request the crypto key from
6 the implantable medical device, and to receive the crypto key from the
7 implantable medical device.

1 63. (previously presented) An apparatus according to Claim 60,
2 wherein the access authentication occurs through a patient designator, further
3 comprising:
4 a short range telemetric connection with the implantable medical device;
5 and
6 the patient designator configured to request the crypto key from the
7 implantable medical device, and to receive the crypto key from the implantable
8 medical device.

1 64. (previously presented) An apparatus according to Claim 60,
2 wherein the access authentication occurs by using a physical token, further
3 comprising:
4 the physical token; and
5 a reader configured to receive the crypto key from the physical token.

1 65. (previously presented) An apparatus according to Claim 60,
2 wherein the implantable medical device maintains patient health information in an
3 unencrypted form and is accessible in the unencrypted form exclusively through a
4 short range telemetric connection.

1 66. (previously presented) An apparatus according to Claim 65,
2 wherein the authenticating with the implantable medical device is through short
3 range telemetry, further comprising:
4 a short range telemetric connection with the implantable medical device;

5 an external source configured to send a session crypto key to the
6 implantable medical device; and
7 an encrypter configured to encrypt the patient health information
8 maintained in the implantable medical device.

1 67. (previously presented) An apparatus according to Claim 60,
2 wherein the access authentication occurs through a patient designator, further
3 comprising:
4 the patient designator configured to establish a short range telemetric
5 connection with the implantable medical device, and to send a session crypto key
6 to the implantable medical device; and
7 an encrypter configured to encrypt patient health information maintained
8 in the implantable medical device.

1 68. (previously presented) An apparatus according to Claim 60,
2 wherein the long range interface is augmented using one or more repeaters.

1 69. (previously presented) A method for securely transacting a data
2 exchange session with an implantable medical device, comprising:
3 maintaining a short range interface device, comprising:
4 providing communication with an implantable medical device; and
5 authenticating access to a securely maintained crypto key using a
6 short range interface; and
7 maintaining an external device, comprising:
8 commencing a data exchange session with the implantable medical
9 device via a long range interface upon successful access authentication; and
10 transacting the data exchange session using the crypto key.

1 70. (previously presented) A method according to Claim 69, wherein
2 the implantable medical device maintains patient health information in an
3 encrypted form.

1 71. (previously presented) A method according to Claim 69, wherein
2 the access authentication occurs through short range telemetry, further
3 comprising:

4 establishing a short range telemetric connection with the implantable
5 medical device;
6 requesting the crypto key from the implantable medical device; and
7 receiving the crypto key from the implantable medical device.

1 72. (previously presented) A method according to Claim 69, wherein
2 the access authentication occurs through a patient designator, further comprising:

3 establishing a short range telemetric connection between the implantable
4 medical device and the patient designator;
5 requesting the crypto key from the implantable medical device; and
6 receiving the crypto key from the implantable medical device.

1 73. (previously presented) A method according to Claim 69, wherein
2 the access authentication occurs by using a physical token, further comprising:

3 accessing the physical token; and
4 receiving the crypto key from the physical token.

1 74. (previously presented) A method according to Claim 69, wherein
2 the implantable medical device maintains patient health information in
3 unencrypted form and is accessible in the unencrypted form exclusively through a
4 short range telemetric connection.

1 75. (previously presented) A method according to Claim 74, wherein
2 the access authentication occurs through short range telemetry, further
3 comprising:

4 establishing a short range telemetric connection with the implantable
5 medical device;
6 sending a session crypto key to the implantable medical device; and

7 encrypting the patient health information maintained in the implantable
8 medical device.

1 76. (previously presented) A method according to Claim 69, wherein
2 the access authentication occurs through a patient designator, further comprising:
3 establishing a short range telemetric connection with the implantable
4 medical device through the patient designator;
5 sending a session crypto key to the implantable medical device; and
6 encrypting the patient health information maintained in the implantable
7 medical device.

1 77. (original) A method according to Claim 69, wherein the long range
2 interface is augmented using one or more repeaters.

1 78. (previously presented) An apparatus for securely transacting a data
2 exchange session with an implantable medical device, comprising:
3 means for maintaining a short range interface device, comprising:
4 means for providing communication with an implantable medical
5 device; and
6 means for authenticating access to a securely maintained crypto
7 key using a short range interface; and
8 means for maintaining an external device, comprising:
9 means for commencing a data exchange session with the
10 implantable medical device via a long range interface upon successful access
11 authentication; and
12 means for transacting the data exchange session by accessing
13 patient health information stored on the implantable medical device using the
14 crypto key.

1 79. (currently amended) An apparatus for securely transacting a data
2 exchange session with an implantable medical device through secure lookup,
3 comprising:

4 a secure server device configured to provide identification of and
5 authentication to access an implantable medical device by authenticating access to
6 a securely maintained crypto key; and
7 a secure external device configured to request the crypto key from the
8 secure server device via a secure short range connection based on the
9 identification of and authentication to access the implantable medical device, to
10 receive the crypto key, to commence a data exchange session with the implantable
11 medical device by transitioning to a long range interface upon successful access
12 authentication, and to transact the data exchange session using the crypto key.

1 80. (currently amended) A method for securely transacting a data
2 exchange session with an implantable medical device through secure lookup,
3 comprising:
4 providing identification of and authentication to access an implantable
5 medical device by authenticating access to a securely maintained crypto key
6 stored on a secure server; and
7 maintaining a secure external device, comprising:
8 requesting the crypto key from the secure server via a secure short
9 range connection based on the identification of and authentication to access the
10 implantable medical device; [[and]]
11 receiving the crypto key;
12 commencing a data exchange session with the implantable medical
13 device by transitioning to a long range interface upon successful access
14 authentication; and
15 transacting the data exchange session using the crypto key.

1 81. (currently amended) An apparatus for securely transacting a data
2 exchange session with an implantable medical device through secure lookup,
3 comprising:

4 means for providing identification of and authentication to access an
5 implantable medical device by means for authenticating access to a securely
6 maintained crypto key stored on a secure server; and
7 means for maintaining a secure external device, comprising:
8 means for requesting the crypto key from the secure server via a
9 secure short range connection based on the identification of and authentication to
10 access the implantable medical device; [[and]]
11 means for receiving the crypto key;
12 means for commencing a data exchange session with the
13 implantable medical device by means for transitioning to a long range interface
14 upon successful access authentication; and
15 means for transacting the data exchange session using the crypto
16 key.